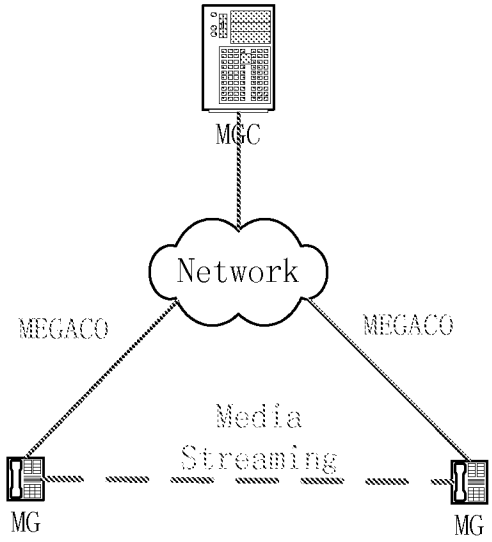
MGC
Network
MEGACO
MEGACO
Media
Streaming
MG
MG

Fig. 1

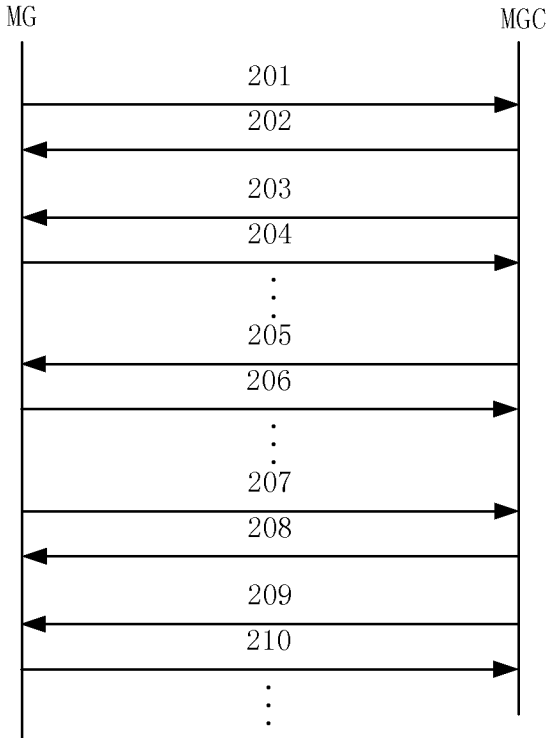
MG
MGC
201
202
203
204
205
206
207
208
209
210

Fig. 2

METHOD OF AUTHENTICATION FOR MEDIA GATEWAY

Technical Field of the Invention

The present invention relates to communication technique, and more particularly, to a method of authentication for Media Gateway with MEGACO/MGCP protocol.

Background of the Invention

Media Gateway Control (MEGACO) protocol is RFC3015 protocol of the Internet Engineering Task Force (IETF).

Fig. 1 shows a system networking diagram for achieving MEGACO protocol. MEGACO protocol employs an idea of separating gateway, which divides a gateway processing signaling and media together into two parts: Media Gateway (MG) and Media Gateway Controller (MGC). MGC controls the operation of MG by MEGACO protocol in such a manner that MGC sends a command to be carried out to MG, and then MG carries it out and returns the result. MGC also processes event requests initiatively sent by MG. Logic relationship in MEGACO protocol is expressed by a connection model. Two basic components of the connection model are contexts and terminations. The context expresses connection and topography relationship between terminations.

Main commands between MGC and MG include SERVICECHANGE, ADD, MODIFY, SUBTRACT, NOTIFY and so on.

In a conventional method of authentication for Media Gateway, after MG registration is finished, MG is authenticated periodically by using a constant key. This has several disadvantages such that firstly if the same key is used for authentication for a long time, it is easy to be decoded by the third party. Secondly, in the method of periodical authentication, it is easy for the third party to make successful authentication between MGC and MG only by filtering the authentication message to

real MG, and initiate a call by forging other MG messages. Thirdly, in the method, only MGC authenticates MG, therefore MG may be called by invalid MGC by forging messages.

Summary of the Invention

One object of the present invention is to provide an improved method of authentication for Media Gateway, which solves the problems in the conventional method of authentication for Media Gateway such that it is easy for the third party to initiate a call by forging MG, to call MG by forging MGC, and to decode the key since the lifetime thereof is short. The method can authenticate each call, update a shared key periodically and prevent calling by using invalid forged messages effectively.

The present invention is achieved by:

The present invention discloses a method of authentication for Media Gateway, comprising: setting up an initial key for validating initial digital signatures between a Media Gateway and a Media Gateway Controller; generating a new shared key having a specific lifetime by performing signaling communication between said Media Gateway and said Media Gateway Controller with said initial key; authenticating calls and responses between said Media Gateway and said Media Gateway Controller with said new shared key; and updating said shared key between said Media Gateway and said Media Gateway Controller if the lifetime of said shared key is expired.

Preferably, the step of generating a new shared key further comprises: initiating a register signaling from said Media Gateway to said Media Gateway Controller to register, wherein said register signaling has a parameter for generating a shared key and a digital signature generated by said initial key; generating a shared key and setting up a lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key; initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said

modification command has a parameter for generating the shared key, a digital signature generated by said initial key and a lifetime of a shared key; and generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

Preferably, the step of authenticating further comprises: for each call, attaching a digital signature to each call message from said Media Gateway Controller to said Media Gateway by using said shared key; validating said digital signature in said call message in said Media Gateway by using said shared key, and if it is valid, returning a response message attached with a digital signature using said shared key to said Media Gateway Controller; and validating said digital signature in said response message in said Media Gateway Controller by using said shared key, if it is valid, setting up a call service, otherwise denying the call.

Preferably, the step of updating said shared key further comprises: sending a notification command from said Media Gateway to said Media Gateway Controller, requesting said Media Gateway Controller to generate a new shared key, wherein said notification command has a parameter for generating a shared key and a digital signature generated by an initial key; generating a new shared key and setting up a lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key; initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said modify command has a parameter for generating the shared key, a digital signature generated by said initial key and the lifetime of the shared key; and generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

Preferably, the algorithm used to generate a shared key by said Media Gateway Controller and said Media Gateway is different from the algorithm used to generate a digital signature by said Media Gateway Controller and said Media Gateway.

Preferably, a field/packet of an expanded protocol is used to transmit said parameter for generating a shared key and said digital signature.

Preferably, the lifetime of said shared key is time, or the number of times said shared key can be used for authentication.

The advantageous effects of the present method are that: the method can not only update a shared key periodically so that it is not easy to decode a key since the key is used for a long time, authenticate each call initiated by MG, and solve the problem that an invalid call is initiated by the third party by filtering messages, but also prevent MG from being called by invalid MGC.

Brief Description of the Drawings

Fig. 1 shows a principle diagram of MEGACO protocol system.

Fig. 2 is a flow chart showing a method of authentication for Media Gateway of the present invention.

Detailed Description of the Preferred Embodiments

The present invention discloses a method of authentication for Media Gateway, comprising:

setting the algorithm used to generate a shared key by a Media Gateway Controller and a Media Gateway is $y=f_1(x)$, and setting the algorithm used to generate a digital signature by a Media Gateway Controller and a Media Gateway is $y=f_2(x)$; the appropriate algorithm can be used for the algorithm used to generate a shared key by a Media Gateway Controller and a Media Gateway and the algorithm used to generate a digital signature by a Media Gateway Controller and a Media Gateway according to the safety level required, and it may not be defined by the present invention.

A key S for validating initial digital signatures is set up between a Media

Gateway and a Media Gateway Controller. The key S of the Media Gateway and the Media Gateway Controller can be different if only it can validate digital signature of the other. A field/packet of an expanded MEGACO protocol can be used to transmit the key and parameter.

A register signaling is initiated from a Media Gateway to a Media Gateway Controller to register, wherein the register signaling has a parameter for generating a shared key and a digital signature. A shared key is generated after the Media Gateway Controller has validated the Media Gateway. A modification command is initiated from the Media Gateway Controller to the Media Gateway, wherein the modification command has a parameter for generating a shared key, a digital signature and a lifetime of a shared key. A shared key is generated after the Media Gateway has validated the Media Gateway Controller.

In subsequent each call and each response between the Media Gateway and the Media Gateway Controller, signatures are attached to each call and each response between the Media Gateway and the Media Gateway Controller by using the shared key. If they are valid after being validated each other, a call service is set up, otherwise the call is denied.

After the lifetime of the shared key is expired, the Media Gateway Controller makes the initial key invalid, and Media Gateway requests the Media Gateway Controller by using a notification command to generate a new shared key and acquire a lifetime of a new key.

The key is thus updated periodically, and calls are authenticated by a new key.

An embodiment of the present invention will be illustrated below by referring the drawings.

Fig. 2 is a flow chart showing a method of authentication for Media Gateway of the present invention. An initial key S is set up between a Media Gateway and a Media Gateway Controller.

201) A register message is initiated from a Media Gateway to a Media Gateway Controller, wherein the register message has a parameter M for generating a shared key by the Media Gateway Controller and a digital signature generated by the key S for the parameter M of the shared key or the register message.

202) The digital signature is validated by using the key S after the Media Gateway Controller receives the message. If it is valid, a shared key S' is generated by using the parameter M of the shared key, and a response is sent to the Media Gateway.

203) A modification message is initiated from the Media Gateway Controller to the Media Gateway, wherein the modification message has a parameter N for generating a shared key by the Media Gateway and a digital signature generated by the key S for the parameter N of the shared key or the whole message, and also has a lifetime of a new shared key wherein the lifetime is time, or the number of times the new shared key can be used for authentication.

204) The digital signature is validated by using the key S after the Media Gateway receives the message. If it is valid, a shared key S' is generated by using the parameter M of the shared key, and a response is sent to the Media Gateway Controller.

205) In a message (such as ADD) set up in subsequent each call, a digital signature is attached by the Media Gateway Controller by using a new shared key S'.

206) The digital signature is validated by using the new shared key S' after the Media Gateway receives the message. If it is valid, the Media Gateway Controller is valid. For a response of the Media Gateway Controller, a digital signature is also attached by using the new shared key S'. The digital signature is validated by using the new shared key S' after the Media Gateway Controller receives. If it is valid, a call is set up, otherwise, the Media Gateway is invalid and the call is denied. The same method is used for the periodical authentication between the Media Gateway and the

Media Gateway Controller.

207) After the lifetime of the shared key set up by the Media Gateway Controller is expired, a notification message is sent from the Media Gateway to the Media Gateway Controller, wherein the notification message has a parameter M' for generating a shared key by the Media Gateway Controller and a digital signature generated by the key S for the parameter M' of the shared key or the whole message.

208) The digital signature is validated by using the key S after the Media Gateway Controller receives the message. If it is valid, a shared key S" is generated by using the parameter M' of the shared key, and a response is sent to the Media Gateway.

209) A modification message is initiated from the Media Gateway Controller to the Media Gateway, wherein the modification message has a parameter N' for generating a shared key by the Media Gateway and a digital signature generated by the key S for the parameter N' of the shared key or the whole message, and also has a lifetime of a new shared key. A new shared key S" is generated by using the parameter N' of the shared key by the Media Gateway, and subsequent calls are authenticated and authenticated periodically by using the new shared key S".

210) A response is sent from the Media Gateway to the Media Gateway Controller.

After the lifetime of the new shared key S" is expired, a new shared key S"' is generated by repeating steps 207)-210), and so on.

While the method of authentication for Media Gateway by using MEGACO protocol has been particularly described with respect to the embodiment thereof, it will be understood by those skilled in the art that many modifications and changes in forms and details may be made without departing from the scope and spirit of the present invention. For example, due to the similarity of MEGACO protocol and MGCP protocol, the technical solution of the present invention is also appropriate for Media

Gateway by using MGCP protocol. It is therefore that the embodiments described above are intended to illustrate but not to limit, and many modifications and changes may fall within the scope of the appended claims.

CLAIMS

1. A method of authentication for Media Gateway, characterized in that the method comprises:

setting up an initial key for validating initial digital signatures between a Media Gateway and a Media Gateway Controller;

generating a new shared key having a specific lifetime by performing signaling communication between said Media Gateway and said Media Gateway Controller with said initial key;

authenticating calls and responses between said Media Gateway and said Media Gateway Controller with said new shared key; and

updating said shared key between said Media Gateway and said Media Gateway Controller if the lifetime of said shared key is expired.

2. The method according to claim 1, characterized in that the step of generating a new shared key further comprises:

initiating a register signaling from said Media Gateway to said Media Gateway Controller to register, wherein said register signaling has a parameter for generating a shared key and a digital signature generated by said initial key;

generating a shared key and setting up a lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key;

initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said modification command has a parameter for generating the shared key, a digital signature generated by said initial key and a lifetime of a shared key; and

generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

3. The method according to claim 1, characterized in that the step of authenticating further comprises:

for each call, attaching a digital signature to each call message from said Media Gateway Controller to said Media Gateway by using said shared key;

validating said digital signature in said call message in said Media Gateway by using said shared key, and if it is valid, returning a response message attached with a digital signature using said shared key to said Media Gateway Controller; and

validating said digital signature in said response message in said Media Gateway Controller by using said shared key, if it is valid, setting up a call service, otherwise denying the call.

4. The method according to claim 1, characterized in that the step of updating said shared key further comprises:

sending a notification command from said Media Gateway to said Media Gateway Controller, requesting said Media Gateway Controller to generate a new shared key, wherein said notification command has a parameter for generating a shared key and a digital signature generated by an initial key;

generating a new shared key and setting up a lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key;

initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said modify command has a parameter for generating the shared key, a digital signature generated by said initial key and the lifetime of the shared key; and

generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

5. The method according to claim 2, 3 or 4, characterized in that the algorithm used to generate a shared key by said Media Gateway Controller and said Media Gateway is different from the algorithm used to generate a digital signature by said Media Gateway Controller and said Media Gateway.

6. The method according to claim 2, 3 or 4, characterized in that a field/packet of an expanded protocol is used to transmit said parameter for generating a shared key and said digital signature.

7. The method according to claim 1, characterized in that the lifetime of said shared key is time, or the number of times said shared key can be used for authentication.

ABSTRACTS

The present invention relates to a method of authentication for Media Gateway, comprising: setting up an initial key for validating initial digital signatures between a Media Gateway and a Media Gateway Controller; generating a new shared key having a specific lifetime by performing signaling communication between said Media Gateway and said Media Gateway Controller with said initial key; authenticating calls and responses between said Media Gateway and said Media Gateway Controller with said new shared key; and updating said shared key between said Media Gateway and said Media Gateway Controller if the lifetime of said shared key is expired. The invention can authenticate each call, update the shared key periodically, and prevent calling invalidly effectively.

Atty. Dkt. No. 006980.00001

Applicant: Kezhi, QIAO, et al.

Title: METHOD OF AUTHENTICATION FOR MEDIA GATEWAY

Appl. No.: 10/566,206

Filing Date: 06/05/2006

Examiner: Unassigned

Art Unit: Unassigned

TRANSLATOR'S DECLARATION

I, the below-named translator, certify that I am familiar with both the Chinese and the English Language, that I have prepared the attached English translation of PCT application no. PCT/CN2003/001069, and that the English translation is a true, faithful and exact translation of the corresponding Chinese language paper.

I further declare that all statements made in this declaration of my own knowledge are true and that all statements made of information and belief are believed to be true; and further, that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of legal decisions of any nature based on them.

August 23, 2007

Date

周心桥

Signature:

ZHOU XINQIAO

Name